REMARKS

This Reply is responsive to the non-final Office Action[1] having a mailing date of October 19, 2006. Claims 1-6 and 8-22 were presented for examination in this second Request for Continued Examination and were rejected. Claims 1, 5, 9, 13, 14 and 22 are independent claims and are amended. No new matter is added. No claims are canceled or added. Thus, claims 1-6 and 8-22 are pending.

Claims 9-13 are rejected under 35 U.S.C. § 101. The Office Action, page 2, alleges that these claims are directed to non-statutory subject matter. Applicants do not necessarily agree with this rejection. Nevertheless, Applicants have amended independent claims 9 and 13 to clearly avoid "101" issues.

Applicants' cryptographic processing programs, as recited in currently amended claims 9 and 13, now recite that those programs are being stored on a computer-readable medium. This amendment is supported by, at least, the disclosure on page 8 of the specification. Furthermore, in claim 13, another change was made to further enhance clarity of the claimed subject matter by reciting the transmitting of the message to the recited memory to invoke a first one of the programs, rather than reciting the transmitting of the message directly to that program.

Applicants submit that currently-amended claims 9-13 are directed to statutory subject matter and that the 35 U.S.C. § 101 rejection should be withdrawn.

[1] The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicants may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicants do not automatically subscribe to, or acquiesce in, any such statement.

Claims 1-6 and 8-22 are rejected under 35 U.S.C. § 103(a) as being un-patentable over Sudia et al. (U.S. Patent No. 5,825,880; hereinafter "Sudia") and further in view of Boebert et al. (U.S. Patent No. 5,596,718, hereinafter "Boebert"). The rejection is respectfully traversed for at least the following reasons.

Consider currently amended claim 1:

> In a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions, comprising: executing an application program at the node which is *not secured*; receiving an input requiring cryptographic-related processing; generating a message via the application program based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component located within the node; transmitting the message to the cryptographic processing component; and performing the cryptographic-related processing by the cryptographic processing component. (Emphasis added.)

Claim 1 calls for, interalia, executing an application program at a node that *is not secured*. Sudia taken alone or in combination with Boebert does not disclose or suggest executing an application program at a node which is not secured, as explained below, after first reviewing some of the claim-change history in this application.

Applicants had previously amended claim 1 by changing "executing an application program at the node which need not be highly secured" to "executing an application program at the node which is not highly secured." Thereafter, that was changed to "executing an application program at the node which is not secured." In turn, that was changed to "executing an application program at the node which is not physically secured." Finally, that is currently amended back to the previous recitation of "executing an application program at the node which is not secured."

Claim 1, therefore, now recites, *interalia*: "executing an application program at the node which is not secured." Against this previously-recited limitation, the previous

office action (May 4, 2006) cited Sudia in view of Veil (6,092,202). Applicants shall discuss this previous rejection below, after first addressing the rejection in the instant Office Action based on Sudia in view of Boebert.

First, consider Sudia. Sudia discloses that a signing device and its associated message server are preferably divided into two physically separate computers (i.e., two separate "nodes"). *See*, at least, Sudia, Fig. 2 and column 7, lines 60-62. Thus, the principal thrust and almost exclusive disclosure of Sudia is to conduct its cryptographic activity on multiple nodes, not in or at one node as recited in Applicants' claims. To attempt to counter this principal, multi-node approach of Sudia, the Office Action finds at least one passage in Sudia which, arguably, can be interpreted as offering single node cryptographic processing in Sudia.

Indeed, in the Office Action, page 5, it says: "Applicant's node is referred in Sudia as the trusted device or known as a smart card or the signing device." In other words, as Applicants can best understand the Office Action, the Examiner is attempting to associate Sudia's "smart card" or the signing device with the single node of Applicants' claims.

Applicants agree that the smart card disclosure in Sudia arguably might have some limited relevance to Applicants' claim 1 because whatever activity which is being performed on that one smart card in Sudia is at least being performed on what might arguably be interpreted as a single node. This, however, requires that the smart card be viewed as a node in the first place. But, the Examiner has provided two contradictory views in this regard. As noted above, on page 5 of the Office Action it suggests that the smart card is "referred in Sudia" to "Applicant's node." But, in complete contradiction,

on page 17 of the Office Action, it says: "A smart card is not considered the node..." The Examiner is requested to clarify this Office Action inconsistency in any subsequent office action if the pending claims are not allowed.

On the one hand, if viewed as a node, then Sudia's smart card may, *arguendo,* be potentially relevant to Applicants' claim 1 which recites that its steps/acts are also being performed in a [single] node. However, any potential relevance goes no further. Consider the following section of Sudia:

> FIG. 3 illustrates a working station for authorizing agents. The human operators who act as authorizing agents may work in relatively unsecured areas at desk-top computers or terminals 51 typically found in a business office. Each such computer or terminal will have a card reader 53, and each operator will have a **secure** "smart card" 55. Each smart card 55 **securely** contains a private decryption key and a private signature key which are unique to that smart card. (Sudia, col. 8, lines 20-27, emphasis added)

This section of Sudia clearly states that the smart card is secure. Since Applicants' claim 1 calls for "executing an application program at the node which is *not secured*" the *secure* smart card disclosure of Sudia (if the smart card is viewed as a node) does not read on this claim element. Sudia's smart card is secure but, quite differently, Applicants' program executing step is executed in a node which is NOT SECURED.

On the other hand, if not viewed as a node, Sudia's smartcard simply does not read on the claim element "executing an application program at the node which is not secured", since it isn't viewed as a node anyway, and the Office Action's position is moot, and need not be addressed herein.

Consider one other section of Sudia:

> As shown, a signing device and its associated message server preferably are divided into two, physically separate computers. Although less preferred, the signing device 39 and message server 47 could be implemented as separate tasks on a single computer in a **highly secure environment.** (Sudia, col. 7, lines 60-65, emphasis added)

This section of Sudia says that to accomplish a single-node constraint for the signing device and its associated message server, A HIGHLY SECURE ENVIRONMENT is needed.

Notably, as shown by the following quotation, even when the signing device and message server of Sudia are separate, as shown in Fig. 2 of Sudia, the signing device is located in a secure location like a vault: "In addition to a signing device 39, each data center configuration 48 additionally contains a *separate* message server 47. The signing device 39 is dedicated to signing operations and is located in a physically secure location, such as a vault." (Sudia, column 7, lines 21-25, Emphasis added.) Thus, even when separate, the signing device is secured, as in a vault. Therefore, if the server and the signing device are on the same computer, the "highly secure environment" requirement noted above must be even more secure than vault security which is used when the server and signing device are separated.

Against this Sudia backdrop of super-security, involving vaults even when the server and signing device are separate, and apparently even more security than that when the server and signing device are on the same computer, consider Applicants' claim 1. Applicants' claim 1 calls for "executing an application program at the node which is *not secured*." Therefore, this section of Sudia clearly does not read on this claim element. In Applicants' single node environment, its recited program executing step is not secured which is the opposite of the highly secure requirement in Sudia.

In view of the above, and as stated multiple times in this prosecution history, Sudia does not read on Applicants' claim 1. Now consider the secondary reference, Boebert.

Boebert discloses a *secure* computer network using a trusted path subsystem which encrypts/decrypts and communicates with a user through local workstation user I/O devices, without utilizing a workstation processor. (Title) Boebert ensures *secure* communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host computer. (Abstract) Boebert is, therefore, principally trying to achieve *secure* communication over a *secure* computer network.

On the one hand, to the extent that Boebert was selected by the Examiner to be cited in direct response to Applicants' usage of the word "physically" in the phrase "not *physically* secure," Boebert should be withdrawn because "physically" has been eliminated from all claims in this current amendment. On the other hand, to the extent that Boebert was cited to suggest that Sudia's requirement for a highly secure environment (for its signing device 39 and message server 47 if implemented as separate tasks on a single computer) can be reduced to non-secure, Applicants disagree. As noted, the purpose of Boebert is to make operations MORE secure, not less.

By combining Boebert with Sudia, assuming they can be combined in the first place (a notion with which Applicants do not necessarily agree), Boebert would only reinforce the notion of Sudia's requirement for a highly secure environment when implementing its signing device and message server on a single node. Boebert would not suggest making Sudia's signing device un-secure; rather, Boebert would suggest making Sudia's signing device MORE secure.

Likewise, to the extent that the Examiner is relying upon Sudia's smart card as a node, which is not clear in view of the two contradictory smartcard positions taken in the

Office Action noted above, Boebert does not dilute the security of Sudia's smartcard. To the contrary, Boebert's purpose of trying to achieve secure communication over a secure computer network suggests, if anything, a higher-security smartcard.

Accordingly, Sudia and Boebert, taken individually or in combination, do not disclose or suggest all elements of claim 1. Namely, they do not disclose or suggest at least: "executing an application program at the node which is not secured" as recited in claim 1. Furthermore, since the remaining steps in claim 1 (receiving, generating, transmitting and performing) are all carried-out in a node that is not secured, then none of these steps can be disclosed or suggested by Sudia and Boebert because the node in Sudia is secured and Boebert, in combination, does not make that node any less secured. Therefore, the 35 U.S.C. §103(a) rejection of claim 1 should be withdrawn and the claim allowed.

PREVIOUSLY APPLIED VEIL REFERENCE:

Next, consider Veil, the previously cited reference, cited in the office action of May 4, 2006 vis-a-vis claim 1. Claim 1 was then worded equally to the currently amended claim 1. Veil also teaches secure transactions in a computer system. (Title and Abstract) Per the May 4, 2006 office action, "Veil teaches an invention for providing secure transaction in a computer system and environments within these transactions (col. 3, line 66 - col. 4, line 3)." (May 4, 2006 office action, page 4, Emphasis added.). Therefore, that office action admits that Veil teaches secure transactions. Nevertheless, despite the teachings of secure transactions in Veil, the Examiner relied on the following section of Veil to support a rejection of the equivalent of the currently-amended claim 1:

> A majority of the application programs for conducting electronic transactions (electronic transactions applications) are executable on one of the conventional operating system platforms such as OS/2.RTM., Windows.RTM., UNIX.RTM. etc. It is generally known that conventional operating system platforms provide a non-secure computing environment for executing the electronic transactions applications. In the non-secure computing environment, confidential information related to the electronic transactions (sensitive data) can be easily compromised. (Veil, column 4, lines 27-36, Emphasis added.)

This section of Veil merely discusses the problem which is allegedly solved by Veil. In other words, the disclosure of Veil overwhelmingly has to do with secure transactions and the provision of a security co-processor to overcome the security deficiency alluded to in the above-quoted section. The above section merely describes the problem that Veil is addressing.

Moreover, this section in Veil discusses no more than conventional operating systems (computer software) which may result in an insecure software environment and therefore carries no weight in countering the *physical-separation* security teachings of Sudia. Indeed, Sudia teaches operational security based on "vaults" and on tamper-proof "smartcards" etc. For example, a principal teaching of Sudia is that the authorizing agent and the signing device are required to be physically separated for security purposes and, as noted above, are separated even to the extent that the signing device is located in a separate physically secure location such as a *vault* (Sudia. Col. 7, lines 24-25, Fig. 2). Security-shortcomings of conventional operating system software performance do not counter this physical-separation security notion.

This physical-separation aspect of security is reinforced throughout Sudia. Consider, for example, "no private signature key exists at a single location where it may

be subject to compromise or catastrophe. Multiple sites must fail or be compromised before interrupting signing services or before an adversary acquires sufficient information to forge signatures." (Sudia, Col. 3, lines 22-27, Emphasis added.) Security-shortcomings of conventional operating system software performance do not counter this physical-separation security notion.

Furthermore, and as noted above with respect to Boebert, Sudia's smart card is touted as being secure: "Each such computer or terminal will have a card reader 53, and each operator will have a *secure* 'smart card' 55. Each smart card 55 *securely* contains a private decryption key and a private signature key which are unique to that smart card." (Sudia, Col. 8, lines 23-27, Emphasis added.) The smart cards are said to be "tamper-resistant." *See*, for example, Sudia, column 3, line 30, or column 9, lines 41-49. Security-shortcomings of conventional operating system software performance do not counter any security notion associated with tamper resistance.

Accordingly, this brief reference in Veil to limitations of conventional operating system platforms allowing a non-secure computing environment does nothing to counter, or offset, the teachings in Sudia of highly secure environments based at least on notions of physical-separation. Conventional operating system performance (computer software operation) has no direct relationship to security based on separate physical locations. Thus, even if these references were combinable, and Applicants do not concede that these references are properly combinable in the first place, their combined teachings would not disclose or suggest the subject matter in Applicants' currently amended claim 1.

Rather, to the contrary, if a combination of the two references were attempted, the secure transaction processing being performed in the security co-processor in Veil, and

any other security discussion in Veil, would actually ADD to the security picture in Sudia. After all, Sudia teaches security and Veil teaches security. In such a case, an augmented security environment resulting from that combination would actually teach away from the "node which is not secured" language recited in Applicants' claim 1. Indeed, the Sudia and Veil references, taken alone or in combination, do not disclose or suggest at least: "executing an application program at the node which is not secured" as recited in claim 1.

Furthermore, since the remaining steps in claim 1 (receiving, generating, transmitting and performing) are all carried-out in a node that is not secured, then none of these steps can be disclosed or suggested by Sudia and Veil because the node in Sudia is secured and Veil, in combination, does not make that node any less secured.

Therefore, Applicants note for the record that any contemplated 35 U.S.C. §103(a) rejection of currently amended claim 1, which the Examiner may be considering, based on a revisiting of the combination of Sudia and Veil, has been previously considered and was previously withdrawn for the reasons given above. Veil should not be re-applied for reasons given above.

Applicants' claim amendment language, "...the node is not secured" is supported by the application as originally filed and as previously discussed on the record. For example, in Applicants' specification, page 6, lines 1-3, it discusses the nodes 110, 120, and 130 of Fig. 1, such nodes along with server 140 and network 150 comprising Applicants' system. As stated therein, those nodes can be any type of computer device. For example, as disclosed therein, those nodes can be "a personal computer, a laptop, a

personal digital assistant (PDA) or a similar device with a connection to network 150." Clearly, these examples of nodes from which Applicants' claimed subject matter can be implemented are not used in a secure environment - e.g., people using a laptop or a PDA do not first find their way to a "vault" and then place themselves with their laptop or PDA inside the vault for security purposes before operating their laptop or PDA. Far to the contrary, laptops and PDA's are used in virtually all public spaces such as, for example, airports, airplanes, trains and train stations, buses and bus depots, taxis, hotels lobbies, corporate business environments, etc. Therefore, Applicants' specification as originally filed clearly supports the notion that the "nodes" of its system are used without their being secured, as recited in amended claim 1.

The other independent claims, claims 5, 9, 13, 14 and 22 each contain a recitation that is the same as, or similar to, the "node which is not secured" language of claim 1. Therefore, these other independent claims, rejected as being un-patentable over the same two references, are allowable for the same, or similar, reasons as those given above with respect to claim 1.

Therefore, claims 2-4 dependent from claim 1, claims 6 and 8 dependent from claim 5, claims 10-12 dependent from claim 9, and claims 15-21 dependent from claim 14 are also allowable, at least for reasons based on their dependencies from allowable base claims.

CONCLUSION

In view of the foregoing claim amendments and remarks, reconsideration and allowance are respectfully requested.

If Applicants receive a final rejection in the next response, in view of the many amendments and explanations that have been placed on the record to date, such final rejection shall signify an impasse to Applicants. Accordingly, Applicants shall respectfully appeal in order to move the prosecution forward.

In summary, Applicants can perform all of their recited cryptographic-related functions at an unsecured node within a network of nodes as claimed while Sudia, taken alone or in combination with any of the cited references, does not disclose or suggest this subject matter.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-2347 and please credit any excess fees to such deposit account.

Respectfully submitted,

By: Eden Stright for Reg 51,208
Joel Wall
Reg. No. 25,648

Date: December 26, 2006

Verizon
Patent Management Group
1515 Courthouse Road, Suite 500
Arlington, VA 22201-2909
Tel: 703.351.3586